AUDITBOARD

A CISO's Strategic Blueprint: Navigating IT and Cyber Risks at the Executive Level

By Richard Marcus

CISOs have long clamored for a seat at the business strategy table, arguing that cyber risks should be front and center when developing and implementing business strategies. With the help of accelerating cyber risk, and mounting regulatory pressures, it seems like that persistence is beginning to pay off. Now, it's critical that we seize this moment to make an impact.

I recently had a lively discussion on this topic with some colleagues from MFC (Nick Stallone, Managing Director; Eric Chan, Director; and Alex Islamov, Director). We explored how CISOs can make the most out of the attention being paid to them by activating, animating and influencing their executive leadership. I want to share some approaches to how we can bridge the gap between the technical world of cybersecurity and the business world of corporate strategy, while being mindful of the potential pitfalls that await us.

Those of us who have been around for a while have witnessed an advancing culture of security awareness over the last 10 years among C-suites and boards. Structures, roles, responsibilities, resourcing, and reporting have elevated infosec to the role where it can collaborate or at the very least contribute to organizational vision, mission, goals, and priorities. This growing consciousness coincides with increasing regulatory pressures and enforcement, which are also good at capturing executive attention.

CISOs can no longer consider cyber risks in isolation. In fact, they are inseparable from other dynamic and volatile sources of uncertainty, such as growth, performance, agility, business continuity, compliance, fraud, third-party dependencies, supply chains, and emerging technology such as artificial intelligence and automation. This ever-changing “VUCA” (volatile, uncertain, complex, ambiguous) landscape means we must continually refresh our contextual awareness and evaluations without suffering from tunnel vision.

But here’s the problem. Full and topical comprehension of an organization’s exposure to cyber risks and appropriate responses requires in-depth technical expertise. How do we communicate that with business executives in terms that will resonate?

Fortunately, most CISOs have a deep appreciation of organizations and their strategies. Once CISOs were simply the geekiest people in the room, but increasingly they are expected to combine their technological prowess with competencies in communication, relationship-building, influence, strategic development, and business management. Many CISOs are capable of sharing an understanding of how risks and controls interact and impact business strategy and decision-making in a way that makes sense to senior leaders. Some opportunities to build alignment with business leadership could include:

- Engage leadership on the topic of anticipated changes to strategic direction. To invoke the great Wayne Gretsky, show them you are “skating to where the puck is going” with your prioritization of risk management strategies.
- Demonstrate how cyber security can be a business enabler by connecting investment in security controls to customer or regulatory requirements that open doors to new markets and revenue opportunities when satisfied.
- Partner with Finance to better understand financial goals and budgetary constraints that help differentiate between “good” risks and “bad” risks based on the language spoken by the business (ex. ROI, Unit Costs, Profit Margin etc)

We must ensure that we prove our relevance. I suggest starting with risk management 101. Risk is the impact of uncertainty on objectives (both positive and negative) and is unavoidable in any goal-oriented activity. In fact, pursuing a goal and taking a risk can be regarded as the same thing. We can demonstrate the tangibility of risks by talking about likelihood and impact, in both qualitative and quantitative terms.

From a shared understanding of risk, we can start explaining the fundamentals of how it is effectively managed. Cyber risk management is simply good risk management, which in turn is just good management. Of course, there are many useful frameworks—e.g., ISO, COSO, NIST, and CIS—all emphasizing the need for a consistent, enterprise-wide approach with clear governance arrangements, objectives, responsibilities, and so on. Leverage the best practices, and the weight of regulatory requirements to make this process and executive relationship tangible and practical.

Before we get carried away in our enthusiasm to gently educate our leaders, we should be mindful of potential pitfalls.

- We can be too technical or not technical enough. Being specific and providing examples helps enormously.
- We make a mistake if we are not honest. By suggesting we start with risk management 101, I am not suggesting we dumb it down. We just need to keep it at a level that aligns with strategic priorities.
- Failure to collaborate is also unhelpful. If we are serious about fomenting an enterprise-wide mindset, we should work with our colleagues in risk management, compliance, internal auditing, and operational management.
- We should avoid being idealistic. Executive leaders will rightly expect us to be pragmatic. Controls add costs, and there are diminishing returns. The aim is not to eliminate risk (which is impossible) but to arrive at an acceptable level and to ensure the organization’s ability to recover.

Above all, our aim as CISOs is to be good business partners that provide continuous value to our executive counterparts. In this role, we can certainly help formulate and communicate a better-informed cyber risk appetite and contribute to value creation and protection. As trust is developed, security leaders have an opportunity to elevate their roles further and meaningfully influence business strategic direction. Fail to influence, or squander that trust, and I’m afraid we will find ourselves back at the kids’ table. But seize this opportunity, and you will be invited back time and time again to make the decisions that matter and foster a risk aware leadership culture.

About the Author

Richard Marcus, CISA, CRISC, CISM, TPECS, is AuditBoard's CISO. He is focused on product, infrastructure, and corporate IT security and leads AuditBoard's internal compliance initiatives. In this capacity, he has become an AuditBoard product power user, leveraging the platform's robust feature set to satisfy compliance, risk assessment, and audit use cases. Connect with Richard on LinkedIn.

About AuditBoard

AuditBoard is the leading cloud-based platform transforming audit, risk, compliance, and ESG management. More than 50% of the Fortune 500 leverage AuditBoard to move their businesses forward with greater clarity and agility. AuditBoard is top-rated by customers on G2, Capterra, and Gartner Peer Insights, and was recently ranked for the fifth year in a row as one of the fastest-growing technology companies in North America by Deloitte. To learn more, visit: AuditBoard.com.